80

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/997,454	11/29/2001	Nikolay Mateev	10011611-1	6153

22879 7590 01/06/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
SHERKAT, AREZOO

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.**	**Applicant(s)**	
	09/997,454	MATEEV ET AL.	
	Examiner	**Art Unit**	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/29/2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *7/30/02 & 3/24/04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Claims 1-24 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4 and 6-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Sheymov, (U.S. Publication No. 2002/0116635 and Sheymov hereinafter).

Regarding claim 1, Sheymov discloses a method for identifying infected program instructions, comprising the steps of:

inserting a dynamic execution layer interface (DELI) between computing device hardware and the program instructions (i.e., Dynamic Decoy Machine and the Code Inspection Management Module)(Page 1, Par 0012 and Page 3, Par. 0037);

monitoring the program instructions as they enter the DELI to determine if the code has been previously processed by the computing device hardware, and when it is the case that the application code has not been previously processed (Page 5, 0049-0050); and analyzing the program instructions to determine if program instructions are infected (i.e., detecting potential malicious code prior to passing code to the protected system)(Page 5, Par. 0049-0060).

Regarding claims 9, 15, and 21, Sheymov discloses a system for detecting infected program instructions in active software applications, comprising:

means for intercepting program instructions, means for determining when the intercepted program instructions have not been processed by the computing device (Pages 5, Par. 0049-0050); and

means for analyzing the intercepted program instructions that have not been processed by the computing device prior to forwarding the intercepted program instructions to computer hardware (i.e., detecting potential malicious code prior to passing code to the protected system)(Page 5, Par. 0049-0060).

Regarding claims 19 and 12-14, Sheymov discloses a computer system, comprising:

a processor, an execution memory (i.e., the protected system)(Page 3, Par. 0035-0037);

a dynamic execution layer interface (DELI)(i.e., Dynamic Decoy Machine and the Code Inspection Management Module)(Page 1, Par 0012 and Page 3, Par. 0037) residing between at least one application and the processor, wherein the DELI comprises: a core configured to cache and execute certain application code fragments, an application programming interface configured to provide access to caching and executing functions of the core to a virus detection manager (i.e., initializing the dynamic decoy machine and updating it if necessary), and a system control and configuration layer configured to provide policies for operation of the core (i.e., actuator module)(Page 5, Par. 0049-0060).

Regarding claim 2, Sheymov discloses wherein the step of analyzing the program instructions comprises an investigation of the contents of instructions within code fragments (Page 5, Par. 0050-0054).

Regarding claim 3, Sheymov discloses wherein the step of analyzing the program instructions comprises inserting decrypted program instructions into a virus detection manager (Page 3, Par. 0032-0034).

Regarding claims 4, 18, 22, and 24, Sheymov discloses further comprising the step of:

releasing program instructions from the virus detection manager when infected program instructions are not detected (Page 5, Par. 0055-0056).

Regarding claim 6, Sheymov discloses wherein the step of analyzing the program instructions comprises monitoring the behavior of the contents of the code fragments in a virtual computing device (Page 3, Par. 0036-0037).

Regarding claims 7 and 20, Sheymov discloses wherein the step of analyzing the program instructions comprises applying a plurality of tests on the contents of the code fragments in a virtual computing device (Page 3, Par. 0036-0037).

Regarding claim 8, Sheymov discloses further comprising the step of:

processing the released program instructions in computer hardware (Page 5, Par. 0055-0056).

Regarding claims 10-11 and 16-17, Sheymov discloses further comprising:

means for gaining control over execution of program instructions (Page 5, Par. 0049-0056).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sheymov, (U.S. Publication No. 2002/0116635 and Sheymov hereinafter), in view of Hypponen et al., (U.S. Patent No. 6,577,920 and Hypponen hereinafter).

Regarding claim 5, Sheymov does not expressly disclose wherein the step of analyzing the program instructions comprises performing a signature comparison with the contents of the code fragments.

However, Hypponen discloses wherein the step of analyzing the program instructions comprises performing a signature comparison with the contents of the code fragments (Col. 4, lines 36-67 and Col. 5, lines 1-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Sheymov with the teachings of Hypponen because it would allow to include the step of analyzing the program instructions comprises performing a signature comparison with the contents of the code fragments with the motivation to scan data being written to or read from a computer's hard disk drive for the presence of macros having a checksum corresponding to one of the identified viruses (Hypponen, Col. 2, lines 1-5).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Nachenberg, (U.S. Patent No. 5,964,889),

Nachenberg, (U.S. Patent No. 5,826,013),

Schnurer et al. (U.S. Patent No. 5,842,002),

Arnold et al., (U.S. Patent No. 5,440,723), Rogers et al., (U.S. Publication No. 2002/0083334), and

Natvig, (U.S. Publication No. 2003/0135791).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat
Arezoo Sherkat
Patent Examiner
Group 2131
Dec. 27, 2004